Supplementary Information for "Quantum key distribution with simply characterized light sources"

Akihiro Mizutani*,[1] Toshihiko Sasaki,[2] Yuki Takeuchi,[3] Kiyoshi Tamaki,[4] and Masato Koashi[2]

[1]Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501 Japan

[2]Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan

[3] NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa 243-0198, Japan

[4] Graduate School of Science and Engineering for Research, University of Toyama, Gofuku 3190, Toyama, 930-8555, Japan

**Mizutani.Akihiro@dy.MitsubishiElectric.co.jp*

In the Supplementary Information, we prove Lemmas 1 and 2 in the main text.

I. PROOF OF LEMMA 1

Lemma 1

$$\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1 \le \lambda\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1 \tag{I.1}$$

with $\lambda := 3+\sqrt{5}$.

Proof. We first explicitly describe $\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1$ and $\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1$ by respectively using Eqs. (18) and (20) in the main text as

$$\begin{aligned}\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1 =& \hat{P}\left[\frac{|001\rangle_A}{\sqrt{2}}\right]\otimes\left(\hat{P}[|1\rangle_B]+\frac{1}{2}\hat{P}[|2\rangle_B]\right)+\hat{P}\left[\frac{|100\rangle_A}{\sqrt{2}}\right]\otimes\left(\frac{1}{2}\hat{P}[|2\rangle_B]+\hat{P}[|3\rangle_B]\right)\\ &+\sum_{s=0}^{1}\hat{P}\left[\frac{|010\rangle_A+(-1)^s|100\rangle_A}{\sqrt{2}}\right]\otimes\hat{\Pi}_{1,s\oplus1}+\sum_{s=0}^{1}\hat{P}\left[\frac{|001\rangle_A+(-1)^s|010\rangle_A}{\sqrt{2}}\right]\otimes\Pi_{2,s\oplus1},\end{aligned} \tag{I.2}$$

$$\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1 = (\hat{P}[|001\rangle_A]+\hat{P}[|100\rangle_A])\otimes\frac{\hat{P}[|2\rangle_B]}{2}+\hat{P}[|010\rangle_A]\otimes(\hat{P}[|1\rangle_B]+\hat{P}[|3\rangle_B]). \tag{I.3}$$

In Eq. (I.2), it is straightforward to show that

$$\sum_{s=0}^{1}\hat{P}\left[\frac{|010\rangle_A+(-1)^s|100\rangle_A}{\sqrt{2}}\right]\otimes\hat{\Pi}_{1,s\oplus1}=\hat{P}\left[\frac{|100\rangle_A|1\rangle_B-\frac{|010\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right]+\hat{P}\left[\frac{|010\rangle_A|1\rangle_B-\frac{|100\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right],$$

$$\sum_{s=0}^{1}\hat{P}\left[\frac{|001\rangle_A+(-1)^s|010\rangle_A}{\sqrt{2}}\right]\otimes\hat{\Pi}_{2,s\oplus1}=\hat{P}\left[\frac{|001\rangle_A|3\rangle_B-\frac{|010\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right]+\hat{P}\left[\frac{|010\rangle_A|3\rangle_B-\frac{|001\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right].$$

To upper-bound $\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1$ by using $\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1$, we remove the four projectors in $\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1$ that are orthogonal to the range of $\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1$, which results in

$$\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1 \ge \frac{1}{2}\left(\hat{P}\left[\frac{|001\rangle_A}{\sqrt{2}}\right]+\hat{P}\left[\frac{|100\rangle_A}{\sqrt{2}}\right]\right)\otimes\hat{P}[|2\rangle_B]+\hat{P}\left[\frac{|010\rangle_A|1\rangle_B-\frac{|100\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right]+\hat{P}\left[\frac{|010\rangle_A|3\rangle_B-\frac{|001\rangle_A|2\rangle_B}{\sqrt{2}}}{\sqrt{2}}\right]. \tag{I.4}$$

Moreover, we apply the following inequality that holds for any normalized vectors $|a\rangle$ and $|b\rangle$ with $\langle a|b\rangle = 0$ [1],

$$\hat{P}\left[|a\rangle - \frac{|b\rangle}{\sqrt{2}}\right] \geq \frac{2}{\lambda}\left(\hat{P}[|a\rangle] + \hat{P}\left[\frac{|b\rangle}{\sqrt{2}}\right]\right) - \hat{P}\left[\frac{|b\rangle}{\sqrt{2}}\right] \tag{I.6}$$

with $\lambda := 3+\sqrt{5}$, to the last two projectors of the rhs in Eq. (I.4) and obtain

$$\begin{aligned}\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1 \geq& \frac{1}{2}\left(\hat{P}\left[\frac{|001\rangle_A}{\sqrt{2}}\right] + \hat{P}\left[\frac{|100\rangle_A}{\sqrt{2}}\right]\right)\otimes \hat{P}[|2\rangle_B]\\ &+\frac{1}{\lambda}\left(P[|010\rangle_A|1\rangle_B] + P\left[\frac{|100\rangle_A|2\rangle_B}{\sqrt{2}}\right]\right) - \frac{\hat{P}[|100\rangle_A|2\rangle_B]}{4}\\ &+\frac{1}{\lambda}\left(P[|010\rangle_A|3\rangle_B] + P\left[\frac{|001\rangle_A|2\rangle_B}{\sqrt{2}}\right]\right) - \frac{\hat{P}[|001\rangle_A|2\rangle_B]}{4}\\ &=\hat{P}_1\hat{e}_{\rm ph}\hat{P}_1/\lambda. \end{aligned}\tag{I.7}$$

This ends the proof of Lemma 1. ■

II. PROOF OF LEMMA 2

Lemma 2 *For any density operator $\hat{\sigma}$,*

$$\mathrm{tr}\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1\hat{\sigma} \leq \mathrm{tr}\hat{e}_{\rm bit}\hat{\sigma} + \sqrt{\mathrm{tr}\hat{\sigma}\hat{P}_1\cdot \mathrm{tr}\hat{\sigma}\hat{P}_3}. \tag{II.1}$$

Proof. From Eq. (19), for any state $\hat{\sigma}$ we have

$$\mathrm{tr}\hat{P}_{\rm odd}\hat{e}_{\rm bit}\hat{P}_{\rm odd}\hat{\sigma} \leq \mathrm{tr}\hat{e}_{\rm bit}\hat{\sigma}, \tag{II.2}$$

which leads to

$$\mathrm{tr}\hat{P}_1\hat{e}_{\rm bit}\hat{P}_1\hat{\sigma} \leq \mathrm{tr}\hat{e}_{\rm bit}\hat{\sigma} - \mathrm{tr}(\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3 + \hat{P}_3\hat{e}_{\rm bit}\hat{P}_1)\hat{\sigma}. \tag{II.3}$$

Since $-\mathrm{tr}(\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3 + \hat{P}_3\hat{e}_{\rm bit}\hat{P}_1)\hat{\sigma} \leq |\mathrm{tr}(\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3\hat{\sigma})| + |\mathrm{tr}(\hat{P}_3\hat{e}_{\rm bit}\hat{P}_1\hat{\sigma})| = 2|\mathrm{tr}(\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3\hat{\sigma})|$ [2], we derive an upper bound on $|\mathrm{tr}(\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3\hat{\sigma})|$. From the expression of the POVM element $\hat{e}^j_{\rm bit}$ given by Eq. (18), we have

$$\hat{T} := 2\hat{P}_1\hat{e}_{\rm bit}\hat{P}_3 = |001\rangle\langle 111|_A \otimes (\hat{\Pi}_{1,1} - \hat{\Pi}_{1,0}) + |100\rangle\langle 111|_A \otimes (\hat{\Pi}_{2,1} - \hat{\Pi}_{2,0}). \tag{II.4}$$

As $(\hat{\Pi}_{1,1} - \hat{\Pi}_{1,0})^2 = (|1\rangle\langle 1| + |2\rangle\langle 2|)/2$ and $(\hat{\Pi}_{2,1} - \hat{\Pi}_{2,0})^2 = (|2\rangle\langle 2| + |3\rangle\langle 3|)/2$, we obtain

$$\begin{aligned}\hat{T}^\dagger\hat{T} =& \hat{P}[|111\rangle_A]\otimes[(\hat{\Pi}_{1,1} - \hat{\Pi}_{1,0})^2 + (\hat{\Pi}_{2,1} - \hat{\Pi}_{2,0})^2]\\ &\leq \hat{I}_{AB}.\end{aligned}\tag{II.5}$$

This inequality implies that the operator norm of $\hat{T}$ is upper-bounded by 1:

$$||\hat{T}||_\infty := \min\{c \geq 0 \text{ s.t. } \forall v\ ||\hat{T}v|| \leq c||v||\} \leq 1, \tag{II.6}$$

where $||\cdot|| := \sqrt{\langle\cdot|\cdot\rangle}$. Next, we define

$$\hat{G} := \hat{P}_3\hat{\sigma}\hat{P}_1. \tag{II.7}$$

---

[1] Note that Eq. (I.6) holds because the smallest eigenvalue of the following Hermitian operator:

$$\hat{P}\left[|a\rangle - \frac{|b\rangle}{\sqrt{2}}\right] - \frac{2}{\lambda}\left(\hat{P}[|a\rangle] + \hat{P}\left[\frac{|b\rangle}{\sqrt{2}}\right]\right) + \hat{P}\left[\frac{|b\rangle}{\sqrt{2}}\right] \tag{I.5}$$

is zero.

[2] The last equality comes from the fact that $|\mathrm{tr}\hat{A}| = |\mathrm{tr}\hat{A}^\dagger|$ holds for any square matrix $\hat{A}$.

Its trace norm $||\hat{G}||_1$ is written by using a unitary operator $\hat{W}$ and is calculated as

$$\begin{aligned} ||\hat{G}||_1 &= |\mathrm{tr}\hat{G}\hat{W}| = |(\sqrt{\hat{\sigma}}\hat{P}_3, \sqrt{\hat{\sigma}}\hat{P}_1\hat{W})| \\ &\le \sqrt{(\sqrt{\hat{\sigma}}\hat{P}_3, \sqrt{\hat{\sigma}}\hat{P}_3)}\sqrt{(\sqrt{\hat{\sigma}}\hat{P}_1\hat{W}, \sqrt{\hat{\sigma}}\hat{P}_1\hat{W})} \\ &= \sqrt{\mathrm{tr}\hat{P}_3\hat{\sigma}}\sqrt{\mathrm{tr}\hat{P}_1\hat{\sigma}}, \end{aligned} \tag{II.8}$$

where we use the definition of Hilbert-Schmidt inner product in the second equality and use Schwarz inequality in the first inequality. Finally, using Hölder's inequality, Eqs. (II.6) and (II.8) gives

$$\begin{aligned} 2|\mathrm{tr}(\hat{P}_1\hat{e}_{\mathrm{bit}}\hat{P}_3\hat{\sigma})| &= |\mathrm{tr}\hat{T}\hat{G}| \le ||\hat{T}\hat{G}||_1 \le ||\hat{T}||_\infty ||\hat{G}||_1 \\ &\le \sqrt{\mathrm{tr}\hat{P}_3\hat{\sigma}\cdot\mathrm{tr}\hat{P}_1\hat{\sigma}}. \end{aligned} \tag{II.9}$$

Therefore, we obtain

$$-\mathrm{tr}(\hat{P}_1\hat{e}_{\mathrm{bit}}\hat{P}_3 + \mathrm{tr}\hat{P}_3\hat{e}_{\mathrm{bit}}\hat{P}_1)\hat{\sigma} \le \sqrt{\mathrm{tr}\hat{P}_1\hat{\sigma}\cdot\mathrm{tr}\hat{P}_3\hat{\sigma}}. \tag{II.10}$$

Finally, by using Eqs. (II.3) and (II.10), we conclude that

$$\mathrm{tr}\hat{P}_1\hat{e}_{\mathrm{bit}}\hat{P}_1\hat{\sigma} \le \mathrm{tr}\hat{e}_{\mathrm{bit}}\hat{\sigma} + \sqrt{\mathrm{tr}\hat{\sigma}\hat{P}_1\cdot\mathrm{tr}\hat{\sigma}\hat{P}_3}. \tag{II.11}$$

This ends the proof of Lemma 2. ■